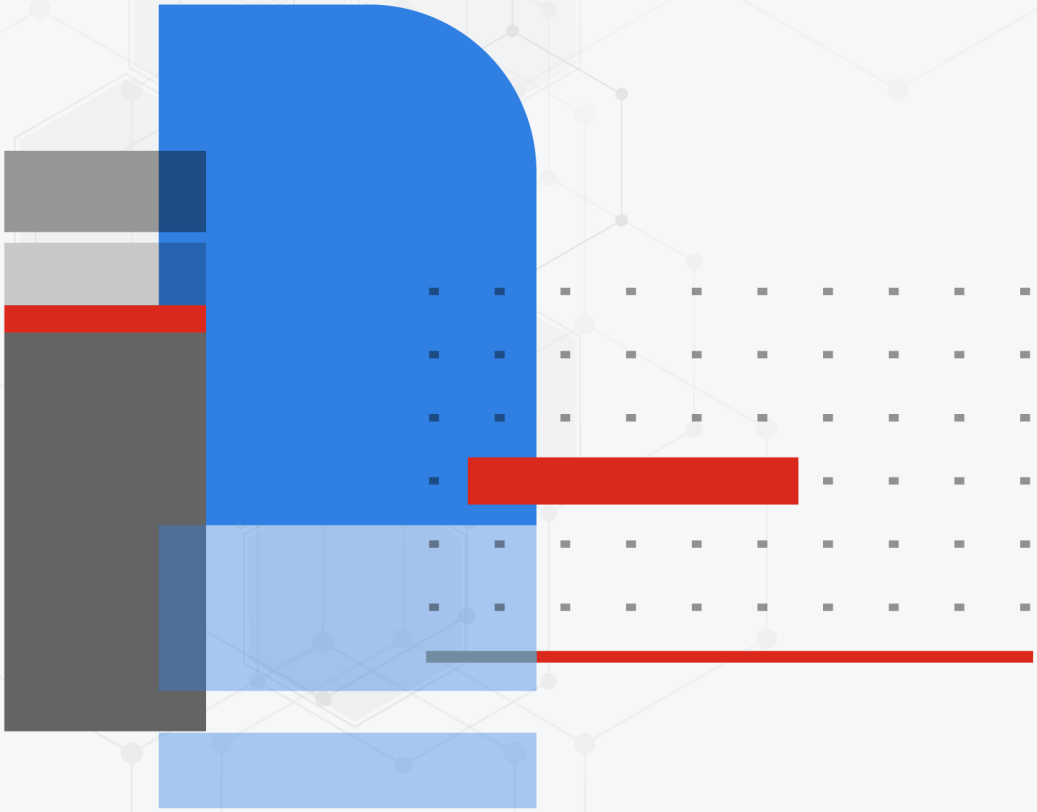
Release Notes

FortiOS 7.4.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 31, 2023
FortiOS 7.4.1 Release Notes
01-741-924847-20230831

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-08-31	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.4.1 build 2463.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.1 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.4.1 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.1 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.1 features.

- FortiGate 6000 incompatibilities and limitations
- FortiGate 7000E incompatibilities and limitations
- FortiGate 7000F incompatibilities and limitations

Remove OCVPN support

The IPsec-based OCVPN service has been discontinued and licenses for it can no longer be purchased as of FortiOS 7.4.0. GUI, CLI, and license verification support for OCVPN has been removed from FortiOS. Upon upgrade, all IPsec phase 1 and phase 2 configurations, firewall policies, and routing configuration previously generated by the OCVPN service will remain. Alternative solutions for OCVPN are the Fabric Overlay Orchestrator in FortiOS 7.2.4 and later, and the SD-WAN overlay templates in FortiManager 7.2.0 and later.

Remove WTP profiles for older FortiAP models

Support for WTP profiles has been removed for FortiAP B, C, and D series models, and FortiAP-S models in FortiOS 7.4.0 and later. These models can no longer be managed or configured by the FortiGate wireless controller. When one of these models tries to discover the FortiGate, the FortiGate's event log includes a message that the FortiGate's wireless controller `can not be managed because it is not supported`.

Remove support for SHA-1 certificate used for web management interface (GUI)

In FortiOS 7.4.0 and later, users should use the built-in Fortinet_GUI_Server certificate or SHA-256 and higher certificates for the web management interface. For example:

```
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

Changes in CLI

Bug ID	Description
913040	The `config vpn ssl settings` option `tunnel-addr-assigned-method` is now available again in the FortiGate 6000 and 7000 CLI. This option had been removed in a previous release because setting this option to `first-available` and configuring multiple IP pools was found to reduce FortiGate 6000 and 7000 SSL VPN load balancing performance. However, some users may want the ability to use multiple IP pools for their SSL VPN configuration, even if performance is reduced. So the change has been reverted.

924384	Rename the `exclude-signatures` setting's `industrial` option to `ot`.
	`config ips global`
	`  set exclude-signatures {none | ot}`
	`end`

924745	Support a new FGCP cluster upgrade mode that allows manual control over the cluster member that is being upgraded. HA members can temporarily run in a multi-version cluster (MVC) while administrators perform tests to confirm traffic can pass through the upgraded member smoothly.
	The syntax for the existing upgrade mode has been changed.
	7.4.0 and earlier:
	`config system ha`
	`  set uninterruptible-upgrade {enable | disable}`
	`end`
	7.4.1 and later:
	`config system ha`
	`  set upgrade-mode {simultaneous | uninterruptible | local-only | secondary-only}`
	`end`
	In `local-only` and `secondary-only` modes, the specific cluster member is upgraded and sessions are synchronized to it. Administrators can manually switch over to the newly upgraded member to test traffic while the cluster operates in MVC. When testing is complete, administrators can manually upgrade the old primary unit.

Changes in GUI behavior

Bug ID	Description
892734	Enhance GUI support for the FortiGuard DLP service by clearly distinguishing DLP dictionaries and sensors that are managed locally and managed by FortiGuard. Use FortiGuard icons for DLP patterns that are dynamically retrieved from FDS.
901387	Update the *System* > *FortiGuard* > *License Information* widget to align with current FortiGuard services and entitlements, as well as corresponding definitions, signatures, engines, and databases associated with each service entitlement.

Changes in default behavior

Bug ID	Description
907096	The IoT Detection service, which includes IoT Detection Definitions (APDB) and the IoT Query service (IOTH), is merged into the Attack Surface Security Rating service (FGSA).
909045	Support enabling one-arm sniffer mode on mirrored ports (RSPAN or ESPAN) between a FortiSwitch port and a FortiGate VLAN interface. Prior to this change, one-arm sniffer mode could only be applied to physical interfaces. After this change, it can be applied to VLAN, VXLAN, and GRE interfaces.
914302	When creating a new `wtp-profile` entry, automatically set `channel-bonding` 40 MHz for 5 GHz radios, and to 160 MHz for 6 GHz radios (FortiWiFi 60E models only).
917647	Support five-digit build numbers for the IPS engine instead of the previous three-digit major/minor version number. When the FortiGate extracts the IPS engine binary, it will now be able to extract IPS engine versions in the five-digit object ID format. Displaying the engine version remains the same in the GUI and CLI, as it already displays the minor version in the five-digit format.
921074	Reposition PSIRT related packages and functionality from the Security Rating entitlement into the Firmware entitlement. This allows more customers with the basic Firmware entitlement to have access to the latest PSIRT package updates, which can be run under *Security Fabric* > *Security Rating* > *Security Posture* checks.

923718	Update SSL VPN default behavior and visibility in the GUI:
	• By default, disable and hide SSL VPN web mode settings from the GUI and the CLI.
	• By default, hide the SSL VPN tunnel mode settings and the *VPN* > *SSL-VPN* menus from the GUI.
	• Divide the CLI configuration settings for VPN GUI feature visibility into IPsec (`set gui-vpn` under `config system settings`) and SSL VPN (`set gui-sslvpn` under `config system settings`), where IPsec is still enabled by default and SSL VPN is now disabled by default.
	• Add warning messages in the GUI on the *VPN* > *SSL-VPN Settings* page under the *SSL-VPN status* and *Authentication/Portal Mapping* fields when SSL VPN tunnel or web mode are enabled.
	• Add a new check on the *Security Fabric* > *Security Rating* page called *Disable SSL-VPN Settings*. This check fails whenever SSL VPN is enabled.
	To enable SSL VPN web mode:
	`config system global`
	`  set sslvpn-web-mode enable`
	`end`
	To enable *VPN* > *SSL-VPN* menus in the GUI:
	`config system settings`
	`  set gui-sslvpn enable`
	`end`

Bug ID	Description
	If SSL VPN web mode and tunnel mode were configured in a FortiOS version prior to upgrading to FortiOS 7.4.1 and later, then the *VPN* > *SSL-VPN* menus and SSL VPN web mode settings remain visible in the GUI. In FortiOS, alternative remote access solutions are IPsec VPN and ZTNA.
930122	Automatic firmware upgrades are now enabled by default on desktop-level FortiGates (100 series and lower). Upgrades will be made to the next stable patch. However, if a FortiGate is part of a Fabric or managed by FortiManager, the `Automatic image upgrade` option is disabled.

Changes in default values

Bug ID	Description
921100	Support HTTPS for SD-WAN performance SLA health checks and change all default HTTP based health-checks to use HTTPS instead. This includes: • Default_AWS • Default_FortiGuard • Default_Google Search • Default_Office_365

New features or enhancements

More detailed information is available in the New Features Guide.

Cloud

See Public and private cloud in the New Features Guide for more information.

Feature ID	Description
912313	When integrating with Cisco ACI using a direct connection SDN connector, allow the ability to filter on the endpoint security group (ESG) when defining and resolving a dynamic address.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description

914305	Improve FortiConverter usability:
	• Highlight the precondition of purchasing a license.
	• Add the ability to hide the FortiConverter prompt when logging in again.
	• Put *Contact Details* as the first step when starting the *Migrate Config with FortiConverter* step.
	• Combine the upload and processing steps, with processing now happening behind the scenes.
	• Add *Administrative distance* option for the management interface.
	• Remove the *Confirm* dialog.
	• Prepopulate the same interfaces in the target configuration.
	• Rename the *FortiConverter Portal* to *FortiConverter Service Portal*.
	• Add *FortiConverter* on the *System* > *FortiGuard* page, regardless of whether the FortiGate has an entitlement or not.
	• Move the FortiConverter option from system to configuration.
	• Display the migrated configuration for review.
	• Automatically back up the original configuration while applying the migrated configuration to the target FortiGate.
	• Add CLI commands:
	  • Use `diagnose sys forticonverter get-prompt-visibility` to see the visibility status of the FortiConverter wizard.
	  • Use `diagnose sys forticonverter set-prompt-visibility {visible | hidden}` to set the visibility status of the FortiConverter wizard.

LAN Edge

See LAN Edge in the New Features Guide for more information.

Feature ID	Description
847106	Support inter-VLAN routing by managed FortiSwitch. This can improve the network performance by offloading Llayer 3 routing from the FortiGate when there is high throughput routing. This feature is particularly beneficial in large production environments, where there are multiple layers of managed FortiSwitches and a vast number of end-user devices. The FortiGate expends a considerable amount of system resources to route traffic between VLANs. This feature enables the FortiGate to offload inter-VLAN traffic between end-users to managed FortiSwitches, freeing up resources on the FortiGate and boosting its performance.
862149	Enhance wireless client mode support on FortiWiFi 80F series models. When wireless client mode is successfully configured and the FortiWiFi local radio has connected to a third-party SSID, this local radio can also concurrently work in AP mode to provide service to wireless clients.
870337	Support GUI *Security Rating* recommendations for multi-chassis link aggregation groups (MCLAGs) up to three tiers, which is an improvement over the previous limitation of only one tier. This allows for more comprehensive security management and configuration of MCLAGs.
888123	Support automatically allowing and blocking intra-VLAN traffic based on FortiLink connectivity status. This feature introduces configuration options to control switch controller access VLAN traffic behavior when the connection to FortiLink is lost. This enables customers to have the option to allow intra-VLAN traffic under the access VLAN on all affected FortiLink until the FortiLink connection is re-established.
893194	Enhance the security of the Security Fabric by supporting authentication and encryption on all Fabric links wherever possible. This protects communication between FortiGate and FortiSwitch devices from unauthorized access and tampering, ensuring its security and integrity. It is supported on FortiLink over L2 and L3 Fabrics to ensure zero touch support.

901576	Simplify BLE iBeacon provisioning whereby the BLE major ID can be set in WTP and WTP group settings (in addition to being set in the BLE profile settings), and the BLE minor ID can be set in the WTP settings (in addition to being set in the BLE profile settings).
	`config wireless-controller wtp`
	`edit <id>`
	`set ble-major-id <integer>`
	`set ble-minor-id <integer>`
	`next`
	`end`
	`config wireless-controller wtp-group`
	`edit <name>`
	`set ble-major-id <integer>`
	`set wtps <wtp-id1>, <wtp-id2>, ...`
	`next`
	`end`

Feature ID	Description
	The BLE major ID defined in the WTP settings overrides the BLE major ID defined in the WTP group settings and the BLE major ID defined in the BLE profile settings. The BLE major ID defined in the WTP group settings overrides the BLE major ID defined in the BLE profile settings. The BLE minor ID defined in the WTP settings overrides the BLE minor ID defined in the BLE profile settings.
905910	Support new changes to the Precision Time Protocol (PTP) configuration on FortiSwitch. This allows FortiOS to manage PTP configuration changes on the FortiSwitch side while maintaining support for previous PTP configuration options.
906431	Before this enhancement, users could be assigned to VLANs dynamically according to the Tunnel-Private-Group-Id RADIUS attribute returned from the Access-Accept message, matching based on a VLAN name table defined under the virtual AP where the VLAN name supported a single VLAN ID. This enhancement allows multiple VLAN IDs to be configured per name tag, up to a maximum of eight VLAN IDs. Once wireless clients connect to the SSID, the FortiGate wireless controller can assign the VLAN ID by a round-robin method from the pool to ensure optimal utilization of VLAN resources.

909971	Support the selection of channels per frequency band for wireless foreground scans when a radio is in monitor mode. This optimizes the wireless foreground scanning operation since only selected channels are scanned.
	`config wireless-controller wids-profile`
	`edit <name>`
	`set ap-scan enable`
	`set ap-scan-channel-list-2G-5G <channel-1> <channel-2> ... <channel-x>`
	`set ap-scan-channel-list-6G <channel-1> <channel-2> ... <channel-y>`
	`next`
	`end`

916757	Enhance wireless client mode support on FortiWiFi 80F, 60F, and 40F series models that allows the local radio to connect with a WPA2/WPA3-Enterprise SSID and support PEAP and EAP-TLS authentication methods.
	`config wifi-networks`
	`edit <id>`
	`set wifi-security wpa-enterprise`
	`set wifi-eap-type {both | tls | peap}`
	`set wifi-username <string>`
	`set wifi-client-certificate <client_certificate>`
	`set wifi-private-key <client_certificate>`
	`next`
	`end`
	The username, client certificate, and private key settings are applicable when connecting to a WPA2/WPA3-Enterprise SSID with EAP-TLS.

Feature ID	Description

920968	Support MIMO mode configuration in the `wireless-controller wtp-profile` on all radios for FortiAP F and G series, and FortiAP-U EV and F series. The MIMO mode configuration setting is added under the radio configuration when creating or editing a `wtp-profile`, and its value range is confined within each AP platform and radio's MIMO specifications (`default`, `1x1`, `2x2`, `3x3`, `4x4`, and `8x8`).
	`config wireless-controller wtp-profile`
	`edit <name>`
	`config radio-<number>`
	`set mimo-mode <supported_modes_depend_on_FAP_platform>`
	`end`
	`next`
	`end`

931695	Integrate with Pole Star's NAO Cloud service by supporting Pole Star BLE asset tags and forwarding their data to the cloud service. This solution allows wearables with BLE asset tags that are worn on staff and guests to communicate with FortiAPs through their built-in Bluetooth radios. The data forwarded to the cloud service is processed by Pole Star, and analytics are generated to map the location of each asset.

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
886560	Support switching to an alternate FortiAnalyzer if the main FortiAnalyzer is unavailable. Once the connectivity is restored, it will automatically fall back to the primary FortiAnalyzer.

928948	Add JSON format support for the syslogd settings.
	`config log syslogd setting`
	`set format json`
	`end`

Network

See Network in the New Features Guide for more information.

Feature ID	Description
730332	Add GUI support for configuring the FortiGate controller and FortiGate connector for the FortiGate LAN extension feature.

Feature ID	Description
733258	Support DNS over QUIC (DoQ) and DNS over HTTP3 (DoH3) for transparent and local-in DNS modes. Connections can be established faster than with DNS over TLS (DoT) or DNS over HTTPS (DoH). Additionally, the FortiGate is now capable of handling the QUIC/TLS handshake and performing deep inspection for HTTP3 and QUIC traffic.
765007	Support network troubleshooting with Connectivity Fault Management (CFM). With CFM, administrators can easily diagnose and resolve issues in Ethernet networks. CFM provides tools for monitoring, testing, and verifying the connectivity and performance of network segments.
829480	The "Happy Eyeballs" (also named fast fallback) algorithm, as outlined in RFC 8305, is supported for explicit web proxy. This feature operates by attempting to connect to a web server that is available at multiple IPv4 and IPv6 addresses, either sequentially or simultaneously. As a result, the web server can be connected with reduced user-visible delay, which enhances the overall browsing experience.
844004	Add GUI support for interfaces with a LAN role, wireless network interfaces, and FortiExtender LAN extension interfaces to receive an IP address from an IPAM server without any additional configuration at the interface level from the *IPAM Settings* tab (*Network* > *IPAM*). IPAM also detects and resolves any IP conflicts that may occur on the interfaces that it manages. If *Auto-resolve conflicts* is disabled in the IPAM settings, the *Reallocate IP* option from the tooltip can be used to manually reallocate the IP address.

865825	Support IPv6 on the cellular interface of FG-40F-3G4G devices.
	`config system lte-modem`
	`set pdptype {IPv4 | IPv6 | IPv4v6}`
	`end`

888381	On FortiGates with a cellular modem and dual SIM support, improve real-time switching to passive SIM when LTE modem traffic exceeds a specified data plan limit for a specified billing period. The SIM switch time occurs shortly after a data plan overage event occurs.
	`config system lte-modem`
	`set data-usage-tracking enable`
	`config sim-switch`
	`set by-data-plan enable`
	`end`
	`config data-plan`
	`edit <id>`
	`set target-sim-slot {SIM-slot-1 | SIM-slot-2}`
	`set data-limit <integer>`
	`set data-limit-alert <integer>`
	`set billing-period {monthly | weekly | daily}`
	`set billing-date <integer>`
	`set billing-weekday {sunday | monday | tuesday | wednesday | thursday | friday | saturday}`
	`set billing-hour <integer>`
	`set overage {enable | disable}`
	`set iccid <SIM_ICCID>`
	`set delay-switch-time <HH:MM>`

Feature ID	Description
	next end end
906748	Webpages can display Cross-Origin Resource Sharing (CORS) content in an explicit proxy environment when using session-based, cookie-enabled, and captive portal assisted authentication. This ensures that webpages are displayed correctly and improves the user experience. config authentication rule edit <name> set web-auth-cookie enable set cors-stateful {enable | disable} set cors-depth <integer> next end
911412	An explicit web proxy can forward HTTPS requests to a web server without the need for an HTTP CONNECT message. The FortiGate explicit web proxy can be configured to detect the HTTPS scheme in the request line of a plain text HTTP request and forward it as an HTTPS request to the web server. This allows applications that cannot use the CONNECT message for sending an HTTPS request to communicate with the web server through an explicit web proxy. config firewall proxy-policy edit <id> set detect-https-in-http-request {enable | disable} next end
912322	Support interfaces belonging to non-management VDOMs to be the source IP of the DNS conditional forwarding server. When `vdom-dns` is disabled, only the IP of the interfaces in the management VDOM can be configured as the source IP. When `vdom-dns` is enabled, only the IP of the interfaces in the current VDOM can be configured as the source IP.
912323	Support the transparent conditional DNS forwarder and add IPv6 support for the conditional DNS forwarder. The transparent conditional DNS forwarder allows the FortiGate to intercept and reroute DNS queries for specific domains to a specific DNS server. This provides greater control over DNS requests, especially when the administrator is not managing the DNS server configuration of the client devices. This can improve network efficiency and performance by resolving IPs local to the client's PCs rather than IPs local to the central DNS server.
916843	The inter-VDOM link is capable of acquiring an IP address from the DHCP server. This allows for more seamless network integration.
928885	Support using the web proxy forward server over IPv6. The new IPv6-enabled forward server works the same way as the previous IPv4 forward server. For example, you can configure an IPv6 address or an FQDN that resolves to an IPv6 address for the forward server, and you can also use the IPv6 forward server in a forward server group.

Feature ID	Description
	config web-proxy forward-server edit <name> set addr-type {ipv6 | fqdn} set ipv6 <IPv6_address> next end

Policy & Objects

See Policy and objects in the New Features Guide for more information.

Feature ID	Description
829983	The enhanced *Policy match* tool retains all the functionality of its predecessor (*Policy lookup*) and adds the ability to return a new policy match results page based on the provided parameters. Policy match results now include web filter profile information (if a web filter is applied) and the ability to use identity-based policy matching. From the *Matched Policy* section in the match results, administrators can redirect to the policy list or edit the policy. The gutter area in the *Policy Match Tool* pane displays the top 10 recent matches. This feature provides a more comprehensive and user-friendly way to diagnose and manage policies. The `diagnose firewall iprope lookup` command has been updated to specify additional parameters, including policy type (policy or proxy), and a new parameter for identity-based policy matching. The policy match feature will be activated if more than six parameters are specified in the existing diagnose command. `# diagnose firewall iprope lookup <source_ip> <source_port> <destination_ip> <destination_port> <protocol> <device> <policy_type> [<auth_type>] [<user/group>] [<server>]`
892953	Support dynamic addresses in security policies in NGFW policy mode. The FABRIC_DEVICE address (a dynamic address consisting of several types of Fabric devices including FortiManager, FortiAnalyzer, FortiClient EMS, FortiMail, FortiAP, and FortiSwitch), can be used as the source or destination address in security policies. The `diagnose ips pme fabric-address list` command can be used to check what address is set in the security policy after FABRIC_DEVICE is used in the address.

915924	Active sessions can be refreshed for specific protocols and port ranges per VDOM in a specified direction. This option can help prevent potential denial of service (DoS) attacks by controlling the direction of traffic that refreshes existing sessions.
	`config system session-ttl`
	`config port`
	`edit <id>`
	`set protocol <integer>`
	`set timeout <timeout_value>`
	`set refresh-direction {both | outgoing | incoming}`

Feature ID	Description
	next end end
920927	The following updates and improvements have been made to the policy list page: • When a single row is selected, display a menu with accompanying descriptive text below it. The *More* dropdown in this menu contains the same items as the right-click context menu. • When multiple rows are selected, the inline menu disappears and the top menu bar changes to display buttons applicable to multi-selection. • Update the top-right view options to a dropdown containing three options. • Add a tooltip to the view option to indicate that selecting *By Sequence* will result in the fastest loading time if the table size is greater than 10 thousand.
923611	Support using tags for dynamic addresses in security policies in NGFW policy mode, including EMS (normal and local EMS tags), FortiPolicy, FortiVoice, and FortiNAC. These tags can be selected as the source or destination addresses in security policies. Once these tags are used in security policies, use the `diagnose ips pme dynamic-address list` command to show the addresses that are used in the policy.

SD-WAN

See SD-WAN in the New Features Guide for more information.

Feature ID	Description

834861	Add route tags to static routes.
	`config router static`
	`edit <seq-num>`
	`set tag <id>`
	`next`
	`end`
	Add password field to BGP neighbor group to be used for the neighbor range.
	`config router bgp`
	`config neighbor-group`
	`edit <name>`
	`set password <password>`
	`next`
	`end`
	`end`

Feature ID	Description
892611	Improve the current SD-WAN neighbor plus `route-map-out-preferable` design to support the multi-PoP multi-hub large scale architecture. In cases where multiple PoPs containing multiple hubs exist, incoming and outgoing traffic to a spoke needs to be preferred over a primary PoP as long as a minimum number of SD-WAN members in the zone meets SLA. When the criteria is not met, then traffic will switch over to a secondary PoP. The following options are added: • `minimum-sla-meet-members` setting in SD-WAN zone configurations • `zone-mode` setting in SD-WAN service configurations • `service-id` attribute in SD-WAN neighbor configurations • `sla-stickness` attribute in SD-WAN service configurations • Allow the `neighbor-group` to be configured under SD-WAN neighbor configurations
893314	The maximize bandwidth (`load-balance`) strategy used prior to FortiOS 7.4.1 is now known as the load balancing strategy. This strategy can be configured under the manual mode and the lowest cost (SLA) strategies. • When the load balancing strategy is configured under the manual mode strategy, SLA targets are not used. • When the load balancing strategy is configured under the lowest cost (SLA) strategy, SLA targets are used.
899827	Improve the client-side settings of the SD-WAN network bandwidth monitoring service to increase the flexibility of the speed tests, and to optimize the settings to produce more accurate measurements. The changes include: • Support UDP speed tests. • Support multiple TCP connections to the server instead of a single connection. • Measure the latency to speed test servers and select the server with the smallest latency to perform the test. • Support the auto mode speed test, which selects either UDP or TCP testing automatically based on the latency threshold.
900198	When a customer using SD-WAN with ADVPN has numerous IPv4 and IPv6 routes per spoke and there are many spokes in the topology, it is more suitable to deploy an IPv4- and IPv6-supported solution without a route reflector that involves an active dynamic BGP neighbor triggered by an ADVPN shortcut. This solution allows a spoke FortiGate to form a BGP neighbor with another spoke FortiGate only after the shortcut tunnel between them has been established. The spoke only learns routes from its BGP neighbors. The following IPv4 and IPv6 BGP configuration settings are required: • The hub FortiGate should be configured with `neighbor-group` and `neighbor-range`/`neighbor-range6`. • Each spoke FortiGate should be configured with `neighbor-group` and `neighbor-range`/`neighbor-range6` (like the hub), and more importantly, each spoke should be configured with `set passive disable` to ensure spokes are able to initiate dynamic BGP connections between each other. • The hub FortiGate should have route reflection disabled (by default) where each `neighbor-group` setting should have `set route-reflector-client disable`.

Feature ID	Description
914659	Add support for the new SD-WAN Overlay-as-a-Service through a license displayed as SD-WAN Overlay as a Service on the FortiGuard page, whose status is updated accordingly. Each FortiGate used with the FortiCloud Overlay-as-a-Service portal must have this license applied to it.

Security Fabric

See Security Fabric in the New Features Guide for more information.

Feature ID	Description
688217	Update FortiVoice Fabric connector: • Display FortiVoice endpoint details in the device tooltips (FortiView monitor and log pages). Users can view the display name and extension number of each FortiFone, making it easier to identify and manage endpoint phones. • When a FortiVoice-supplied MAC or IP address is used in a firewall policy, automatically create a FortiVoice tag (MAC/IP) dynamic address on the FortiGate that contains all the provisioned FortiFones registered with FortiVoice. The dynamic address can be used in firewall policies to restrict rules to authorized FortiFones only.
860248	Add CIS security control mappings to the *Security Rating* page. Users can view ratings by CIS compliance and view the description for each CIS control. The FortiGate must have a valid Attack Surface Security Rating license to view security ratings grouped by CIS.
875696	Add prompting for a one-time upgrade when a critical vulnerability is detected upon login. After logging in, the GUI displays a warning message about the critical vulnerability and allows the administrator to either upgrade or skip it. This ensures that the administrator is aware of any potential security risks and can take immediate action to address them.

Security Profiles

See Security profiles in the New Features Guide for more information.

Feature ID	Description
780874	OT virtual patching is a method for mitigating vulnerability exploits against OT devices by applying patches virtually on the FortiGate. In short, when a virtual patching profile is enabled on a firewall policy, the IPS engine will use the MAC address of the device to verify whether known vulnerabilities and mitigation rules are associated with it. If there is, then the IPS engine will apply mitigation rules to traffic for that device.

Feature ID	Description
819093	The inline CASB security profile enables the FortiGate to perform granular control over SaaS applications directly on firewall policies. The supported controls include privilege control, safe search, tenant control, and UTM bypass. Administrators can also customize their own SaaS applications, matching conditions, and custom controls and actions. A firewall policy must use proxy-based inspection with a deep inspection SSL profile in order to apply inline CASB and scan the traffic payload.
869769	Display application signatures in a hierarchical manner when defining application overrides in the GUI.
915879	Add two FortiGuard web filter categories: • Artificial intelligence technology (category 100): sites that offer solutions, insights, and resources related to artificial intelligence (AI). • Cryptocurrency (category 101): sites that specialize in digital or virtual currencies that are secured by cryptography and operate on decentralized networks.
925363	The FortiGate can download quarantined files in an archive format (.TGZ) instead of the original raw file. This allows for a more detailed analysis of the quarantined files and reduces the risk of malware infection.

System

See System in the New Features Guide for more information.

Feature ID	Description
739200	Add GUI support to prevent FortiGates with an expired support contract from upgrading to a major or minor firmware release.
843997	Support Enrollment over Secure Transport (EST) and the RFC 7030 standards when generating a new CSR request, performing automatic renewals, or manually regenerating a certificate. EST provides more security for automatic certificate management than Simple Certificate Enrollment Protocol (SCEP), which is commonly used for certificate enrollment. `# execute vpn certificate local generate est <options>`
905629	Introduce the Operational Technology (OT) Security Service to help consolidate OT services under one license and to decouple the underlying definitions and packages from IoT ones. New OT-related services such as OT Detection Definitions and OT Virtual Patching Signatures used in the virtual patching profile are now licensed under the OT Security Service.
909935	Include a built-in entropy token source, which eliminates the need for a physical USB entropy token when booting up in FIPS mode on any platform. This enhancement meets the requirements of FIPS 140-3 Certification by changing the source of entropy to jitter entropy, which is known for its reliability and security.
914674	Support log rotation for `auto-script`. Upon reaching its maximum size, the log file will seamlessly begin overwriting from the start, rather than halting the script.

Feature ID	Description
927945	Introduce selected availability (SA) versioning and labeling for special builds provided for customers that will remain on the build for a long duration. The SA versioning uses an odd number as the minor version, and a four-digit number for the patch version.

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description
743804	Add a RADIUS option to allow the FortiGate to set the RADIUS accounting message group delimiter to a comma (,) instead of a plus sign (+) when using RSSO. The default delimiter is still a plus sign.
885400	Support local user password policies with enhanced complexity options. This allows customization of the local firewall user password policy with various settings, such as minimum length, character types, and password reuse. These settings are similar to the ones available for the system administrator password policy, which offers more security and flexibility than the previous local user password policy. After upgrading, users must activate the user password policy using the CLI. The previous password policy settings will remain valid, but they will not be effective unless the password policy is enabled. If the password policy is not enabled, the `expire-days <integer>` option will not force users to change their password after number of specified days.
932769	Allow secure connections to SSL VPNs using certificate-based authentication. By utilizing the RADIUS protocol for authorization, access is granted based on the content of the Subject Alternative Name (SAN) in the user's certificate. This adds an extra layer of security by ensuring that only users with valid certificates can access the VPN.

VPN

See IPsec and SSL VPN in the New Features Guide for more information.

Feature ID	Description
780297	Enhance IKE debug filtering: • Reorganize `ike-log-filter` and `ike-gateway-filter` into two separate sub-commands. • Rename the `src-addr` and `dst-addr` filter options to `loc-addr` and `rem-addr` to make the naming more precise. • Add option to show the name of current executing functions in the IKE debug log (`diagnose vpn ike log function-name {enable | disable}`). • Display VDOM name instead of VDOM index in the debug log to provide more readability.

Feature ID	Description

881903	Adjust the DTLS heartbeat parameters for SSL VPN. This improves the success rate of establishing a DTLS tunnel in networks with congestion or jitter.
	`config vpn ssl settings`
	`set dtls-heartbeat-idle-timeout <integer>`
	`set dtls-heartbeat-interval <integer>`
	`set dtls-heartbeat-fail-count <integer>`
	`end`
	The default value for these attributes is 3 seconds, which is also the minimum allowable value. The maximum allowable value for these attributes is 10 seconds.

884772	Securely exchange serial numbers between FortiGates connected with IPsec VPN. This feature is supported in IKEv2, IKEv1 main mode, and IKEv1 aggressive mode. The exchange is only performed with participating FortiGates that have enabled the `exchange-fgt-device-id` setting under `config vpn ipsec phase1-interface`.
909970	Support multiple interface monitoring for IPsec. This enables IPsec to monitor multiple interfaces per IPsec tunnels and activate the backup link only when all primary links are down. This is useful for customers who have more than one WAN link and want to minimize the use of their LTE or 5G interfaces, which are more costly and bandwidth-intensive. This allows customers to optimize their WAN link selection and performance, and reduce their operational expenses.

ZTNA

See Zero Trust Network Access in the New Features Guide for more information.

Feature ID	Description
913238	Add four new categories and 14 subtypes of ZTNA replacement messages that correspond to new error codes error messages. Additional information is displayed for specific errors, and provides end users with more information about the error encountered.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.4.1 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.1
FortiManager	• 7.4.1
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 and later
FortiAP	• 7.2.2 and later
FortiAP-U	• 6.2.5 and later
FortiAP-W2	• 7.2.2 and later
FortiClient* EMS	• 7.0.3 build 0229 and later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 and later
FortiClient* Mac OS X	• 7.0.3 build 0131 and later
FortiClient* Linux	• 7.0.3 build 0137 and later
FortiClient* iOS	• 7.0.2 build 0036 and later
FortiClient* Android	• 7.0.2 build 0031 and later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 4.2.0 and later for post-transfer and inline scanning

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.4.0, use FortiClient 7.4.0.

Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor
18. FortiPolicy

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.4.1. When Security Fabric is enabled in FortiOS 7.4.1, all FortiGate devices must be running FortiOS 7.4.1.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account

- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*.

FortiGate 6000 and 7000 upgrade information

Upgrade FortiGate 6000 firmware from the management board GUI or CLI. Upgrade FortiGate 7000 firmware from the primary FIM GUI or CLI. The FortiGate 6000 management board and FPCs or the FortiGate 7000 FIMs and FPMs all run the same firmware image. Upgrading the firmware copies the firmware image to all components, which then install the new firmware and restart. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

On a standalone FortiGate 6000 or 7000, or an HA cluster with `uninterruptible-upgrade` disabled, the firmware upgrade interrupts traffic because all components upgrade in one step. These firmware upgrades should be done during a quiet time because traffic can be interrupted for a few minutes during the upgrade process.

Fortinet recommends running a graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Fortinet recommends that you review the services provided by your FortiGate 6000 or 7000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.4.1:

1. Use the following command to set the `upgrade-mode` to `uninterruptible` to support HA graceful upgrade:

```
config system ha
    set uninterruptible-upgrade enable
end
```

When upgrading from FortiOS 7.4.1 to a later version, use the following command to enable uninterruptible upgrade:

```
config system ha
    set upgrade-mode uninterruptible
end
```

2. Download the FortiOS 7.4.1 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.
5. Confirm that all components are synchronized and operating normally.
   For example, go to *Monitor* > *Configuration Sync Monitor* to view the status of all components, or use `diagnose sys confsync status` to confirm that all components are synchronized.

IPS-based and voipd-based VoIP profiles

In FortiOS 7.4.0 and later, the new IPS-based VoIP profile allows flow-based SIP to complement SIP ALG while working together. There are now two types of VoIP profiles that can be configured:

```
config voip profile
    edit <name>
        set feature-set {ips | voipd}
    next
end
```

A voipd-based VoIP profile is handled by the voipd daemon using SIP ALG inspection. This is renamed from proxy in previous FortiOS versions.

An ips-based VoIP profile is handled by the IPS daemon using flow-based SIP inspection. This is renamed from flow in previous FortiOS versions.

Both VoIP profile types can be configured at the same time on a firewall policy. For example:

```
config firewall policy
    edit 1
        set voip-profile "voip_sip_alg"
        set ips-voip-filter "voip_sip_ips"
    next
end
```

Where:

- `voip-profile` can select a `voip-profile` with `feature-set voipd`.
- `ips-voip-filter` can select a `voip-profile` with `feature-set ips`.

The VoIP profile selection within a firewall policy is restored to pre-7.0 behavior. The VoIP profile can be selected regardless of the inspection mode used in the firewall policy. The new `ips-voip-filter` setting allows users to select an IPS-based VoIP profile to apply flow-based SIP inspection, which can work concurrently with SIP ALG.

Upon upgrade, the `feature-set` setting of the `voip profile` determines whether the profile applied in the firewall policy is `voip-profile` or `ips-voip-filter`.

Before upgrade	After upgrade
config voip profile edit "ips_voip_filter" set feature-set flow next edit "sip_alg_profile" set feature-set proxy next end config firewall policy edit 1 set voip-profile "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end	config voip profile edit "ips_voip_filter" set feature-set ips next edit "sip_alg_profile" set feature-set voipd next end config firewall policy edit 1 set ips-voip-filter "ips_voip_ filter" next edit 2 set voip-profile "sip_alg_profile" next end

Product integration and support

The following table lists FortiOS 7.4.1 product integration and support information:

Web browsers	• Microsoft Edge 112 • Mozilla Firefox version 113 • Google Chrome version 113 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 112 • Mozilla Firefox version 113 • Google Chrome version 113 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 0311 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2022 Standard
	  • Windows Server 2022 Datacenter
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Novell eDirectory 8.8

AV Engine	• 7.00018
IPS Engine	• 7.00509

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions

Citrix Hypervisor	• 8.2 Express Edition, CU1
Linux KVM	• Ubuntu 22.04.3 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• Windows Server 2019
Windows Hyper-V Server	• Microsoft Hyper-V Server 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 113 Google Chrome version 112
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 112
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 112
macOS Ventura 13.1	Apple Safari version 16 Mozilla Firefox version 103 Google Chrome version 111
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 7.4.1. To inquire about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
857718	*Return Email DNS Check* in the email filter profile is case sensitive.

Anti Virus

Bug ID	Description
908706	On the *Security Profiles* > *AntiVirus* page, a VDOM administrator with a custom administrator profile cannot create or modify an antivirus profile belonging to the VDOM.

Data Leak Prevention

Bug ID	Description
911291	The FortiGate does not parse the entries of the sensor from DLP signature package properly, and therefore cannot block files matching a sensor as expected.

Endpoint Control

Bug ID	Description
808737	FortiOS should pull new avatar API from EMS and handle the avatar status on the FortiGate.

Explicit Proxy

Bug ID	Description
817582	When there are many users authenticated by an explicit proxy policy, the *Firewall Users* widget can take a long time to load. This issue does not impact explicit proxy functionality.
859693	Session state is incorrectly shown as `SYN_SENT` when using an IP pool in explicit proxy policy.
890776	After upgrading a FWF-61F, get configuration error and the `gui-explicit-proxy` setting is lost.

Firewall

Bug ID	Description
708229	ACL feature is incorrectly dropping fragmented UDP packets.
843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI. This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.
847715	A VIP group having members of the FQDN and static NAT VIP types cannot be created using the GUI (*Policy & Objects* > *Virtual IPs* page).
872312	Unable to add more MAC addresses once the MAC address group object for a VWP policy referenced.
895946	Access to some websites fails after upgrading to FortiOS 7.2.3 when the firewall policy is in flow-based inspection mode.
910068	On the *Policy & Objects* > *Firewall Policy* page, if any of the interface names contain a space, the page does not load when *Interface Pair View* is selected.
912740	On a FortiGate managed by FortiManager, after upgrading to 7.4.0, the *Firewall Policy* list may show separate sequence grouping for each policy because the `global-label` is updated to be unique for each policy.
917495	When editing a VLAN ID, the FortiGate deletes firewall policies but does not recreate them again if the interface is in a zone.
919418	On the *Policy & Objects* > *Firewall Policy* page, when the interface name used in a virtual wire pair is a substring of interfaces used in a firewall policy, such policies are not displayed. For example, if a virtual wire pair consists of interfaces port1 and port2, firewall policies with port10, port11, port21, port22 are not displayed.
929138	The *Edit Address* page does not load if the address name contains has special characters ([ ]).

FortiGate 6000 and 7000 platforms

Bug ID	Description
888310	The FortiGate 6000 or 7000 front panel does not appear on the *Network* > *Interfaces* and *System* > *HA* GUI pages.
888447	In some cases, the FortiGate 7000F platform cannot correctly reassemble fragmented packets.
888873, 909160	The FortiGate 7000E and 7000F platforms do not support GTP and PFCP load balancing.
891430	The FortiGate 6000 and 7000 *System Information* dashboard widget incorrectly displays the management board or primary FIM serial number instead of the chassis serial number. Use `get system status` to view the chassis serial number.
897629	The FortiGate 6000 and 7000 platforms do not support EMAC VLANs.
899905	Adding a FortiAnalyzer to a FortiGate 6000 or 7000 Security Fabric configuration from the FortiOS GUI is not supported.
902545	Unable to select a management interface LAG to be the direct SLBC logging interface.
905692	On a FortiGate 6000 or 7000, the active worker count returned by the output of `diagnose sys ha dump-by group` can be incorrect after an FPC or FPM goes down.
905788	Unable to select a management interface LAG to be the FGSP session synchronization interface.
908576	On a FortiGate 7000F, after a new FPM becomes the primary FPM, IPsec VPN dynamic routes are not synchronized to the new primary FPM.
908674	Sessions for IPsec dialup tunnels that are configured to be handled by a specific FPC or FPM may be incorrectly sent to a different FPC or FPM, resulting in traffic being blocked.
913040	Multiple IP pools in SSL VPN is not supported.
918795	An uncertified warning appears only on the secondary chassis' FIM02 and FPMs.
921452	After an SNMP HA failover, the SNMP trap continues to work.

FortiView

Bug ID	Description
808384	Real-time FortiView *Traffic Shaping* monitor shows 0 bandwidth for active FTP traffic.

GUI

Bug ID	Description
562570	*System* > *FortiGuard* page's *License Information* table does not show the updated IPS engine version.
825598	A `Node exiting due to unhandled rejection: TypeError [ERR_INVALID_URL]: Invalid URL` error message appears in the debug crash log for the node process. This error does not impact the GUI operation.
857464	The *CPU* and *Sessions* widgets report the current numbers at the wrong places for most time periods.
863126	In an environment where the Security Fabric is enabled and there are more than 100 firewall object conflicts between the root and downstream FortiGates, the *Firewall Object Synchronization* pane does not list the details.
892364	Incorrect interface is being selected in the *SD-WAN Rules* GUI page, but the correct one is displayed in the CLI.
893560	When private data encryption is enabled, the GUI may become unresponsive and HA may fail to synchronize the configuration.
897004	On rare occasions, the GUI may display blank pages when the user navigates from one menu to another if there is a managed FortiSwitch present.
898386	Browser returns a blank page after logging in to the GUI with an IPv6 address.
898902	In the *System* > *Administrators* dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the *Two-factor Authentication* toggle. This issue does not affect configuring other settings in the dialog.
903856	When using configuration save mode with VDOMs, the GUI still shows unsaved changes after another administrator commits their changes with SSH.
905200	When logged in to the GUI of a non-management VDOM and trying to complete the *Migrate Config with FortiConverter* step in the startup menu, the page does not update and the loading spinner is stuck.
905795	Random FortiSwitch is shown as offline on the GUI when it is actually online.
914176	GUI should allow user to skip the *Migration Config with FortiConverter* step without having to wait for a server connection.
920881	Improve the policy list performance.

HA

Bug ID	Description
703614	HA secondary synchronization fails and keeps rebooting when the primary has a split port configuration.
771316	Platforms in an HA environment get stuck in a reboot loop while attempting to synchronize configurations that differ in split ports.
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.
858683	FortiGate in A-P HA mode with `admin-restrict-local` enabled allows the local administrator to log in to the passive host, even if LDAP is available.
908062	FortiGate VM Azure HA cluster goes out-of-sync due to dynamic firewall address type.
916903, 919982, 922867	When an HA management interface is configured, the GUI may not show the last interface entry in `config system interface` on several pages, such as the interface list, policy list, address list, and DNS servers page. This is a GUI-only display issue and does not impact the underlying operation of the affected interface.
920233	The *System* > *HA* page is missing from the GUI on 5K models.

Hyperscale

Bug ID	Description
832924	Timeouts occur when accessing the Migros Bank e-banking application and https://www.gs***.ch/ when the session is offloaded.
915796	With an enabled hyperscale license, in some cases with exception traffic (like ICMP error traverse), the FortiGate may experience unexpected disruptions when handling the exception traffic.

Intrusion Prevention

Bug ID	Description
810783	The number of IPS sessions is higher than kernel sessions, which causes the FortiGate to enter conserve mode.
823583	Failover on clustered web application using keepalived daemon does not work seamlessly.

IPsec VPN

Bug ID	Description
664828	L2TP VPN not working when offloading is enabled.
780297	IKE debug log filtering functionality exhibits inaccuracies, resulting in the possibility of displaying unmatched logs when filters are set.
803010	The `vpn-id-ipip` encapsulated IPsec tunnel with `npu-offload` cannot be reached with IPv6.
883138	VM running FIPS cipher mode does not show AES-CBC ciphers when configuring IPsec in the GUI.
885333	Forwarded broadcast traffic on ADVPN shortcut tunnel interface dropped.
899822	IPsec dialup tunnel interface does not appear in the *Interface* dropdown of a *Dashboard* > *Status* > *Interface Bandwidth* widget.
923061	With ICMPv6 ff02::1, all nodes' addresses experience incrementing IPsec TX errors.

Log & Report

Bug ID	Description
831441	The forward traffic log show exabytes of data being sent and received from external to external IP addresses in multiple VDOMs.
839934	Destination interface in traffic log does not match the SD-WAN quality description in the log details.
860822	When viewing logs on the *Log & Report* > *System Events* page, filtering by *domain\username* does not display matching entries.
906888	Free-style filter not working as defined under `config fortianalyzer override-filter`.

Proxy

Bug ID	Description
733258	Support HTTP3 for web proxy and ZTNA web service.
783549	An error condition occurs in WAD caused by multiple outstanding requests sent from client to server with UTM enabled.
820096	CPU usage issue in proxyd caused by the absence of TCP teardown.

REST API

Bug ID	Description
886012	The MTU value on an interface cannot be set using the interface REST API.

Routing

Bug ID	Description
775752	`link-down-failover` does not bring the BGP peering down.
849988	The *Network* > *SD-WAN* > *SD-WAN Rules* page does not show a red exclamation mark for addresses that have `dst-negate` enabled. This is cosmetic; users can use the CLI to confirm that the address has `dst-negate` enabled.
907386	BGP neighbor group configured with password is not working as expected.
924940	When there are a lot of policies (several thousands), the interface member selection for the *SD-WAN Zone* dialog may take up to a minute to load.

Security Fabric

Bug ID	Description
862424	On a FortiGate that has large tables (over 1000 firewall policies, address, or other tables), security rating reports may cause the FortiGate to go into conserve mode.
874822	In a configuration with a connected FortiAP-U, the *FortiAP & FortiAP-S & FortiAP-W2 & FortiAP-U Command Injection in CLI* security rating test fails and suggests an upgrade to 7.0.4, even though the FortiAP is on the latest version (7.0.0).
876422	After adding a 20 MB blocklist file, a FortiGate with 2 GB RAM goes to conserve mode when viewing the *Security Fabric* > *External Connectors* page.
907172	Automation stitch with FortiDeceptor Fabric connector event trigger cannot be triggered.

SSL VPN

Bug ID	Description
719740	The *No SSL-VPN policies exist* warning is displayed when an SSL VPN zone having an SSL VPN tunnel interface is used in a policy. The warning can be ignored; it does not affect the SSL VPN functionality.
822657	Internal resource pages and menus are not showing correctly in web mode.
830068	SSL VPN stops listening on IPv6 interface after a reboot.
835014	Webpage keeps loading when customer accesses an internal webpage in the SSL VPN web portal.
843756	Customer bookmark (*.tr***.pt) is not accessible when using SSL VPN web mode.
845817	Jira application is not loading properly when connecting through SSL VPN web mode.
851976	PC cannot get IP from DHCP server due to `find duplicate ip` and causes the dialup SSL VPN to fail.
854607	In SSL VPN web mode, the page keeps loading after logging in.
859275	Issues with accessing an internal site using SSL VPN web mode and bookmark.
881268	Disconnecting from SSL VPN using the *SSL-VPN* widget does not disconnect the SSL VPN tunnel.

922446	SSL VPN service over PPPoE interface does not work as expected if the PPPoE interface is configured with `config system pppoe-interface`.
	`config system pppoe-interface`
	`  edit <name>`
	`  set device <string>`
	`  set username <string>`
	`  set password <password>`
	`  next`
	`end`
	
	`config vpn ssl settings`
	`  set source-interface <PPPoE_interface_name>`
	`end`
	
	This issue is also observed on VNE tunnel configurations.

Switch Controller

Bug ID	Description
848632	Upon upgrade, the link to FortiSwitch stays down with QSFP.

Bug ID	Description
861227	On the *WiFi & Switch Controller* > *FortiSwitch Ports* page, the *Device Information* column lists the same device multiple times.
902338	*WiFi & Switch Controller* > *FortiSwitch Ports* page does not show VLANs exported to another tenant VDOM, which results in the VLAN being removed if saved from the GUI.
904640	When a FortiSwitch port is reconfigured, the FortiGate may incorrectly retain old detected device data from the port that results in an unexpected number of detected device MACs for the port. Using `diagnose switch-controller mac-cache show` to check the device data can result in the *Device Information* column being blank on the *WiFi & Switch Controller* > *FortiSwitch Ports* page or in the *Assets* widget.
911232	Security rating shows an incorrect warning for unregistered FortiSwitches on the *WiFi & Switch Controller* > *Managed FortiSwitches*.

System

Bug ID	Description
708964	CPU usage issue is observed caused by reloading the system when the system has `cfg-save` set to `revert`.
713951	Not all ports are coming up after an LAG bounce on 8 × 10 GB LAG with ASR9K. Affected platforms: FG-3960E and FG-3980E.
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled.
766834	High memory usage caused by downloading a large CRL list.
801481	Download speed issue through WAN configured with PPPoE on FortiGate.
802932	CPU usage issue caused by clearing BGP dampened prefixes.
816579	User loses GUI/SSH access on FG-1500D while running one-arm sniffer.
820559	When backing up the configuration to a USB disk, if the file name is the same as specified under *System* > *Settings* > *Start Up Settings* > *USB auto-install*, an *Invalid file name* error is displayed.
828557	FortiGate as DHCP relay is not showing a DHCP decline in the debugs when there is an IP conflict in the network.
836748	FG-100F fails to boot when FortiOS image binary is larger than 94 MB.
855573	False alarm of the PSU2 occurs with only one installed.
873391	If the FortiGate is added to FortiManager using the IPv6 address and tunnel is down for some reason, the FortiGate will not reconnect to FortiManager since `fmg` under `system central-management` is not set properly.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.

Bug ID	Description
884023	When a user is logged in as a VDOM administrator with restricted access and tries to upload a certificate (*System* > *Certificates*), the *Create* button on the *Create Certificate* pane is greyed out.
887940	Status light is not showing on the FortiGate 60F or 100F after a cold reboot.
900670	QSFP/QSFP+ port23/port24 are down after upgrading to 7.0.11 on FG-3401E.
904486	False alarm message, `fos_ima: fos_process_appraise 99: Suspicous Executable File(/data/bin/node) is missing hash`, might be shown and then forces the FortiGate to reboot.
909345	An error condition occurs caused by receiving ICMP redirect messages.
910651	On FG-600F, all members are up but the LACP status is showing as down after upgrading.
923364	System goes into halt state with `Error: Package validation failed...` message in cases where there are no engine files in the FortiGate when the BIOS security level is set to 2.
923834	The DSL modem on the firewall does not work after the device starts.
925657	After a manual system administrator password change, the updated `password-expire` is not received by the FortiManager auto-update.
933277	The `npu-vdom-link` cannot forward the traffic after the first two packets.
944581	Checksum on FortiOS is different from md5sum.txt file on the InfoSite when upgrading from previous GA build.

User & Authentication

Bug ID	Description
738846	FAS ends up in an endless loop while synching with LDAP due to special character (,) as part of the username.
868481	When the *Guest User Print Template* is customized in a VDOM, printing the guest user credentials from *User & Authentication* > *Guest Management* still uses the default *Guest User Print Template*.
891068	Guest administration management does not show all groups for multiple VDOMs assigned to a guest administrator account.
896739	SSO administrator configuration breaks with Azure Cloud due to `config system saml` having a trailing slash in the metadata link.
915192	Device detection sometimes does not identify the correct IP addresses of devices.
922133	Unable to view authorization page on FortiGate pop-up when the pre-login and post-login banner are set on FortiGate while using OAuth authorization.
923164	EAP proxy daemon may keep reloading after updating the certificate bundle.
929112	RADUIS server dialog in the GUI incorrectly changes the custom RADUIS port to 0.

VM

Bug ID	Description
902816	An error condition occurs after a failover on the HA cluster deployed on an FG-VM64-AZURE.
912184	An error condition is observed after deploying an FG-VM64-AZURE in Standard_DS4_v2 size.
924689	FortiGate VMs in an HA cluster deployed on the Hyper-V platform may get into an unresponsive state where multiple services are impacted: GUI management, CLI commands, SSL VPN sessions, DHCP assignment, traffic throughput, and reboot function.

Web Filter

Bug ID	Description
873086	On the *Policy & Objects* > *Security Policy* page for a policy-based VDOM, adding an external threat feed category to the *URL Category* field does not apply the changes.
885222	HTTP session is logged as HTTPS in web filter when VIP is used.

WiFi Controller

Bug ID	Description
873273	The *Automatically connect to nearest saved network* option does not work as expected when FWF-60E client-mode local radio loses connection.
877609	RADIUS COA does not work in some cases.
896128	Some 5 GHz weather channels should not be allowed in certain countries.
904349	Unable to create FortiAP profile in the GUI for dual-5G mode FortiAP U231F/U431F models.
905406	In `auth-logon` and `auth-logout` logs, Wi-Fi users with random public IP addresses are observed.
921456	FAP-431F is deauthenticating clients after roaming when DHCP enforcement is enabled on the SSID, even when the client gets IP from DHCP.
930130	MPSK keys are not loaded completely in the wpad daemon after applying a VAP with an MPSK profile selected on a FortiAP.
938525	Roaming is not working on FAP-431Fs for WPA2 enterprise bridge SSID with FortiNAC.

ZTNA

Bug ID	Description
828433	FortiAuthenticator Cloud zero trust tunnel (ZTNA connection) fails when EMS Fabric connector is configured.

Known issues

The following issues have been identified in version 7.4.1. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

FortiGate 6000 and 7000 platforms

Bug ID	Description
885205	IPv6 ECMP is not supported for the FortiGate 6000F and 7000E platforms. IPv6 ECMP is supported for the FortiGate 7000F platform.
887946	UTM traffic is blocked by an FGSP configuration with asymmetric routing.
891642	FortiGate 6000 and 7000 platforms do not support managing FortiSwitch devices over FortiLink.
892499	IPv6 SD-WAN service rules are not supported on 6KF and 7KE models. 7KF models are not impacted.
892844	In a FortiGate 6000 and 7000 FGCP cluster, when logged into the secondary FortiGate, the *System Information* dashboard widget incorrectly displays the serial number of the primary FortiGate instead of the serial number of the secondary FortiGate. Use `get system status` to view the serial number of the secondary FortiGate.
896758	Virtual clustering is not supported by FortiGate 6000 and 7000 platforms.
905450	SNMP walk failed to get the BGP routing information.
907140	Authenticated users are not synchronized to the secondary FortiGate 6000 or 7000 chassis when the secondary chassis joins a primary chassis to form an FGCP cluster.
907695	The FortiGate 6000 and 7000 platforms do not support IPsec VPN over a loopback interface or an NPU inter-VDOM link interface.
910606	FortiGate 6000 or 7000 FGCP session synchronization may not synchronize all sessions.
910824	On the FortiGate 7000F platform, fragmented IPv6 ICMP traffic is not load balanced correctly when the `dp-icmp-distribution-method` option under `config load-balance` is set to `dst-ip`. This problem may also occur for other `dp-icmp-distribution-method` configurations.
910883	The FortiGate 6000s or 7000s in an FGSP cluster may load balance FTP data sessions to different FPCs or FPMs. This can cause delays while the affected FortiGate 6000 or 7000 re-installs the sessions on the correct FPC or FPM.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
912778	FortiGate 6000 and 7000 graceful upgrade from FortiOS 7.0.11 (and older versions) to 7.4.0 is not supported. After upgrading to 7.4.0, all or part of the configuration may be lost.

Bug ID	Description
	Workaround: upgrade to 7.4.0, reset the FortiGate to factory defaults, and then redo the configuration.
937879	FortiGate-7000F chassis with FIM-7941Fs cannot load balance fragmented IPv6 TCP and UDP traffic. Instead, fragmented IPv6 TCP and UDP traffic received by the FIM-7941F interfaces is sent directly to the primary FPM, bypassing the NP7 load balancers. IPv6 ICMP fragmented traffic load balancing works as expected. Load balancing fragmented IPv6 TCP and UDP traffic works as expected in FortiGate-7000F chassis with FIM-7921Fs.

GUI

Bug ID	Description
907041	*Network* > *SD-WAN* > *SD-WAN Zones* and *SD-WAN Rules* pages do not load if a shortcut tunnel is triggered. **Workaround**: to load the *Network* > *SD-WAN* page, temporarily bring down the ADVPN shortcut tunnels, go to the *Network* > *SD-WAN* page, and bring it back up after.

HA

Bug ID	Description
947210	Multiple instances of `*** code requested backtrace ***` for SSL VPN daemon observed during a graceful upgrade (on FG-6000F).

Hyperscale

Bug ID	Description
896203	The parse error, `NPD-0:NPD PARSE ADDR GRP gmail.com MEMBER ERR`, appears after rebooting the system.
936747	Connections per second (CPS) performance of SIP sessions accepted by hyperscale firewall policies with EIM and EIF disabled that include overload with port block allocation (PBA) GCN IP pools is lower than expected. **Workaround**: enter the following command for each NP7 processor to resolve the performance issue. `# diagnose npu np7 setreg <npu_#> nss.nss_thrd_ctrl.thrd_ctrl 0xF` Where `<npu_#>` is the NP7 processor number. NP7 processors are numbered 0, 1, 2, and so on.

Bug ID	Description
	The configuration changes from entering these diagnose commands are reset if the FortiGate restarts. After a system restart, just re-enter the diagnose commands.

IPsec VPN

Bug ID	Description
916260	The IPsec VPN tunnel list can take more than 10 seconds to load if the FortiGate has large number of tunnels, interfaces, policies, and addresses. This is a GUI display issue and does not impact tunnel operation.

Routing

Bug ID	Description
903444	The `diagnose ip rtcache list` command is no longer supported in the FortiOS 4.19 kernel.

SSL VPN

Bug ID	Description
933985	FortiGate as SSL VPN client does not work on NP6 and NP6XLite devices.

System

Bug ID	Description
899279	NP7 did not offload jumbo packet, but get `NPU INFO: offload=9/9` in the console output.
907622	GUI is missing DDNS *Domain* text field box when creating a new DDNS entry.
912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using `execute reboot` command) with an SD card inserted.
939110	DHCP server on LAN interface is lost after rebooting or restoring the configuration file.
942502	Kernel panic occurs when creating EMAV VLAN interfaces based on an aggregate interface with new kernel 4.1.9.

Bug ID	Description
948448	A super_admin administrator is unable to log in after restoring the VDOM configuration on the admin VDOM and rebooting the FortiGate.

User & Authentication

Bug ID	Description
823884	When a search is performed on a user *(User & Authentication > User Definition* page), the search results highlight all the groups the user belongs to.
884462	NTLM authentication does not work with Chrome.

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the *Managed FortiAPs* page and *FortiAP Status* widget can take a long time to load. This issue does not impact FortiAP operation.
869978	CAPWAP tunnel traffic over tunnel SSID is dropped when offloading is enabled.
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP (over 50). This issue does not impact FortiAP management and operation.
944465	On the *WiFi & Switch Controller > Managed FortiAPs* page of a non-root VDOM, the *Register* button is unavailable in the *Device Registration* pane.
946796	The eap_proxy daemon may keep reloading randomly due to failing to bind a port. This will cause an IKE and WiFi authentication failure. **Workaround**: stop sflowd.

Built-in AV engine

Resolved engine issues

Bug ID	Description
886780	Explicit proxy does not block MSI file type in file filter.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
835757	IPS Engine 6.004.133 crashes with signal 11.
845954	FortiGate with the flow-based AV enters conserve mode during the BP test (1G interfaces).
864118	XFF does not always populate in the IPS logs.
872747	CPU utilization reaches 99% due to IPS process and ipsengine has a signal 11 crash.
886685	IPS engine has high memory usage.
889464	VDOM limit of IPS custom signature is 1000, but 1000 is showing as the global limit.
897523	Issues occur with TCP SACK and TCP retransmissions by IPS/NTurbo when DPI is used.
902857	FortiGate does not forward TLS ServerHello to client when IPS is enabled with flow mode and deep inspection.
905636	Azure Machine Learning instances fail to load with flow-based inspection.
908682	First HTTPS attempt with infected EICAR file cannot be blocked by IPS Engine 7.166 in a flow mode AV profile.
910002	DNS translation does not work as expected after disabling *Log all DNS queries and responses* (`set log-all-domain disable`).
912577	DNS queries (A/AAAA) from Linux have timeouts and delays.
916992	DNS static filter does not work as expected if it is the only setting in the DNS profile.
923836	Deep inspection and flow mode does not work for certain URLs.
932111	IPS engine memory leak results in difference between FortiOS memory and IPS memory.
937578	IPS engine crashes after upgrading to 7.0.12.
938937	IPS and AV engines crash.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com